Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

System Fundamentals

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Chapter Outline

- Background
- OSI Model & TCP/ IP Suite
- Subnetting, Ports, and DNS
- Networks Devices
- Networks Security

Background

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

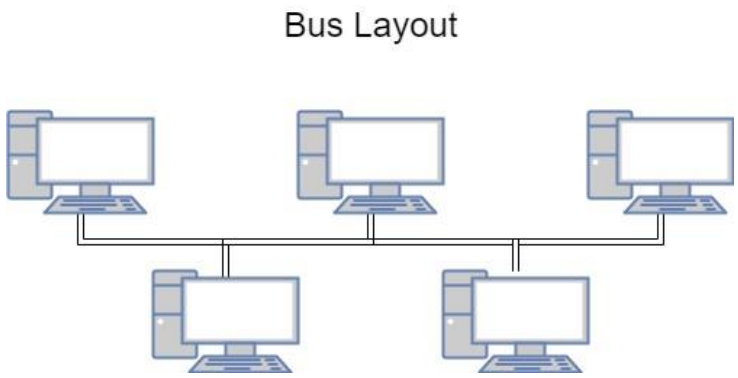
Ervin, Kelly and Lee, William

Networking Topology

- Network topology is the layout of the network both logical and physical.
- Logical layout is how the network is accessed and the flow of data.
- Physical layout deals with the positioning and wiring used to connect devices together. Some examples are:
  - Bus
  - Ring
  - Star
  - Mesh
  - Hybrid

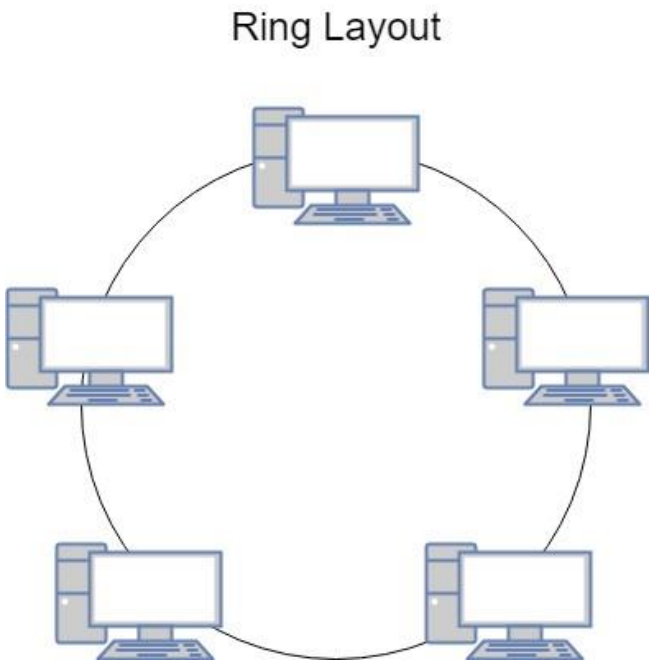
Bus Layout

- **The bus layout is the simplest layout and places all nodes in a single connection line.**
  - **Data must enter at node one and go through each node until it reaches its destination.**
  - **One issue is that if node 2 then node 3, 4, 5, etc. lose connectivity as well.**



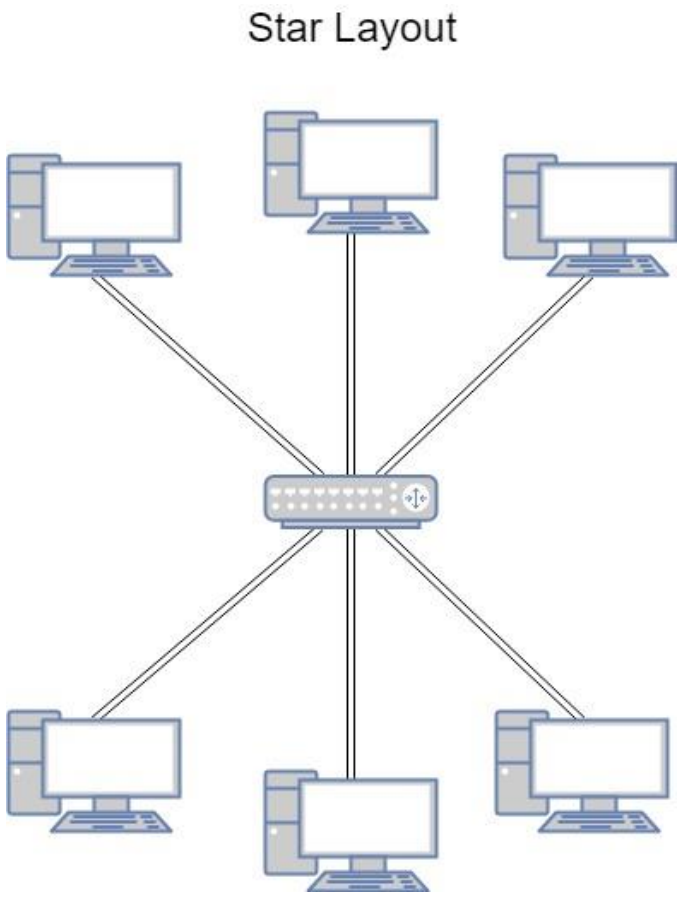
Ring Layout

- **The ring layout mitigates the bus vulnerability by connecting the last node to the starting node.**
  - **This creates a loop, which allows proper data transfer even if one node loses connection.**



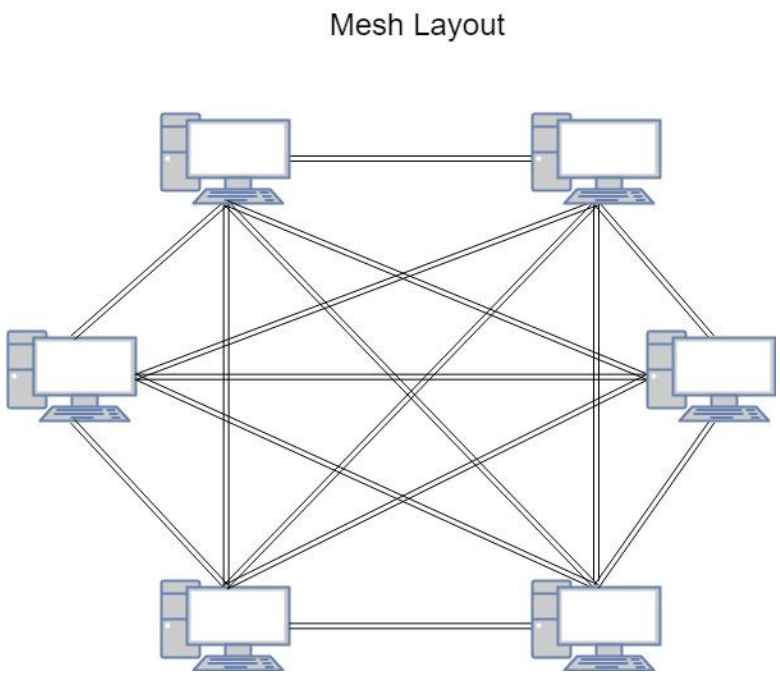
Star Layout

- **The star layout has one central switch or hub connects several devices.**
  - **The most common layout.**
  - **Nodes can go offline without effecting the other nodes in the network.**
  - **If the switch or hub goes offline then the entire network loses connectivity.**



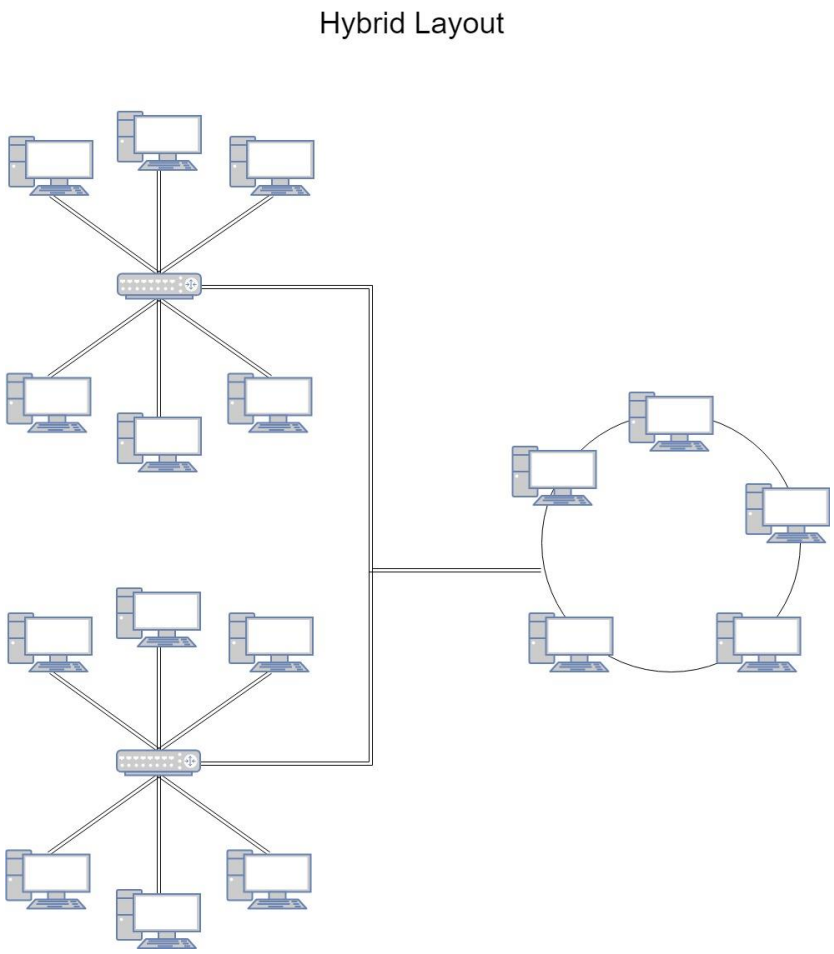
Mesh Layout

- **The mesh layout has a spider web like design. Each node has multiple paths to reach each other .**
  - **These redundant connections allow the system to reduce the effect of outages.**
  - **Used for mission critical services.**
  - **Troubleshooting issues can be difficult.**



Hybrid Layout

- **The hybrid layout is a mix of any of the previous layouts being used together.**
  - **Many modern setups use a hybrid layouts.**
  - **These layouts try to combine the best aspects of each layouts.**



OSI Model & TCP/ IP Suite

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Open Systems Interconnection Model

- **The OSI model is a framework used to maximize the compatibility between software, systems, and protocols.**
  - **OSI Model Layers**
    - **Physical Layer**
    - **Data Link Layer**
    - **Network Layer**
    - **Transport Layer**
    - **Session Layer**
    - **Presentation Layer**
    - **Application Layer**

OSI Model Layers

- **Layer 1: Physical**
  - **Consists of physical devices like ethernet cables, fiber optic cables, microwave transmission, etc.**
    - **Attacks on this level consists of wire tapping and other physical methods of intercepting data.**
- **Layer 2: Data link**
  - **Encompasses basic ethernet and Wi-Fi protocols. Handles linking of IP address to MAC address. Handles the transfer of data and ensures that it is received without errors.**
- **Layer 3: Network**
  - **Based on the routing protocol and current factors this layer decides the delivery path of data packets. IP addressing occurs at this layer.**

OSI Model Layers

- **Layer 4: Transport**
  - **Makes sure that the transport of data is successful by using error checking techniques and maintaining the data sequence.**
    - **Both the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are used in this layer.**
- **Layer 5: Session**
  - **A system session is a persistent connection between two devices. This layer identifies, monitors and controls these sessions. It also manages multiple connections and separate connections to different resources.**
    - **Connecting to a computer remotely is an example of a system session.**

OSI Model Layers

- **Layer 6: Presentation**
  - **Incoming data is translated into a format that can be understood by the application layer. Encryption methods like Secure Sockets Layer (SSL) can be applied in this layer.**
    - **Layer 6 presents information to Layer 7**
- **Layer 7: Application**
  - **Specifies the standard communication interface and protocols used by software processes. This gives these processes access to the network.**
    - **Common protocols like FTP and HTTP are used in this layer.**

TCP/ IP Suite

- **The TCP/ IP Suite is complimentary to the OSI model. It helps track where data is in the traffic flow process.**
  - **TCP/ IP Suite Layers**
    - **Network Interface Layer**
    - **Internet Layer**
    - **Host-to-Host Transport Layer**
    - **Application Layer**

TCP/ IP Suite Layers

- **Layer 1: Network Interface**
  - **Packets are prepared for transmission. IP address is linked to the MAC address. Defines basic ethernet and Wi-Fi protocols**
    - **Equivalent to layer 1 and layer 2 of the OSI model.**
- **Layer 2: Internet**
  - **Decides the delivery path of data packets based on given parameters and protocols.**
    - **Equivalent to layer 3 of the OSI model.**

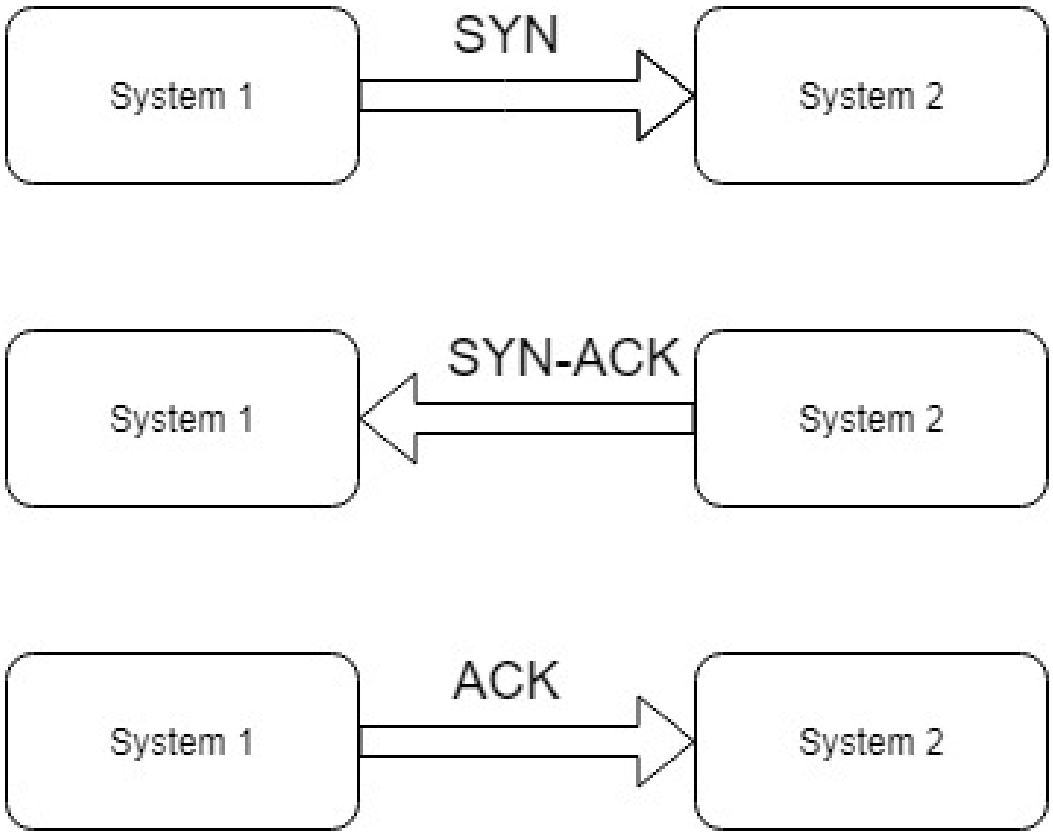
TCP/ IP Suite Layers

- **Layer 3: Host-to-Host Transport**
  - **Works on transmitting the data either through TCP or UDP protocol.**
    - **Equivalent to layer 4 of the OSI model.**
- **Layer 4: Application**
  - **This layer performs tasks similar to layer 5, layer 6, and layer 7 of the OSI model.**

TCP 3 Way Handshake

- **TCP is a connection oriented protocol. It establishes a connection and verifies that packets are sent to the destination successfully.**
  - **First the sending system notifies the second system it would like to initiate communication with a SYN packet.**
  - **Then the receiving system sends back an ACK (acknowledgment) packet with a SYN.**
  - **Finally the sending systems sends one last ACK packet to signify that it is ready for TCP communication.**

3 Way Handshake Example



Subnetting, Ports, and DNS

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

IP Subnetting

- An IP address is a numerical label for each device in a network. It is used for location addressing and to identify the device.
- Subnetting is the division of a physical network into two or more logical networks.
  - This conserves IP addresses, reduces network traffic, and simplifies the network.

Hex, Binary, and Decimal

- **Converting between hex, binary, and decimal is an important skill and could potentially be on the CEH exam.**

Hex	Binary	Decimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10

Ports

- **Ports allow computers to send data. It is the connection point to an external or internal device.**
  - **Many ports are associated with a particular protocol or application.**
  - **Range 1 – 1023: Has several common, well known protocols.**
  - **Range 1024 – 49151: Has ports that are regularly registered by applications for specific tasks.**
  - **Range 49152 – 65535: Are free ports that can be used for any TCP or UDP traffic.**

Significant Ports & Uses

Port	Use
20 – 21	FTP
22	SSH
23	Telnet
25	SMTP
42	WINS
53	DNS
80, 8080	HTTP
88	Kerberos
110	POP3
111	PortMapper (Linux)

Port	Use
123	NTP
135	RPC-DCOM
139	SMB
143	IMAP
161, 162	SNMP
389	LDAP
445	CIFS
514	Syslog
636	Secure LDAP
1080	Socks5

Port	Use
1241	Nessus Server
1433, 1434	SQL Server
1494, 2598	Citrix Application
1521	Oracle Listener
2512, 2513	Citrix Management
3389	RDP
6662 – 6667	IRC

Ports

- **Ports allow computers to send data. It is the connection point to an external or internal device.**
  - **Many ports are associated with a particular protocol or application.**
  - **Range 1 – 1023: Has several common, well known protocols.**
  - **Range 1024 – 49151: Has ports that are regularly registered by applications for specific tasks.**
  - **Range 49152 – 65535: Are free ports that can be used for any TCP or UDP traffic.**

Domain Name System

- The DNS main function is to convert names into IP addresses (157.166.226.26 → www.cnn.com).
- The top level servers include the addresses of the DNS servers for the top level domains (.com, .org, etc.)
- Many modern infrastructures may not work without DNS.

Networks Devices

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Routers and Switches

- **Routers are used to connect networks together.**
  - **Its main function is to direct level 3 traffic packets to a specific location depending on the network address.**
  - **They also use Network Address Translation, which allows several internal devices to share one external IP address.**
- **Switches create multiple broadcast domains.**
  - **They deliver data based on the MAC address of the device.**
  - **These devices commonly operate on layer 2.**

Proxies and Firewalls

- **Proxies sit between the internal system and the outside world, which prevents them from communicating directly.**
  - **They operate on layer 7 and can be used to filter outgoing traffic.**
  - **Another benefit is their ability to cache website data.**
- **Firewalls are usually defined as three types: packet filtering, stateful packet filtering, and proxies.**
  - **Packet filtering firewalls use rules to allow or disallow specific packets based on the header information.**
  - **Stateful packet filtering determines the legitimacy of traffic by the state of the connection.**

Network Security

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Intrusion Prevention/ Detection

- **Intrusion detection systems (IDS) are meant to detect any suspicious network activity.**
  - **Once suspicious activity is detected it will attempt to alert the administrator or owner of the network.**
- **Intrusion Prevention Systems (IPS) behave similarly to an IDS, but in addition to sending a notification they try to disrupt the activity.**

Backups and Archiving

- The archive bit says whether a file has been changed or not since the last backup. This is how systems decide if a file needs to be backed up again.
- There are three different types of backups:
  - A full backup resets all archive bits and backs up everything.
  - A differential backup only backs up files that have changed since the last full backup but does not reset the archive bit.
  - An incremental backup only backs up files that have changed since the last full backup or last incremental backup. Afterwards it does reset the archive bit.